

REMARKS

Claims 24, 28, 30, 33-35, 37, and 40-51 are pending. Claims 24, 28, 30, 33-35, 37, and 50-51 are rejected under 35 USC 103(a) as being unpatentable over U.S. patent 7,215,775 (Noguchi et al.) in view of U.S. patent 6,947,559 (Gleeson). Claims 40-45 are rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson and U.S. patent application publication 2002/0154769 (Petersen et al). Claim 46 is rejected under 35 USC 103(a) as being unpatentable over Noguchi in view of Gleeson, and in view of Petersen, and in view of U.S. patent 6,973,499 (Peden).

Claim 44 is canceled. Claims 24, 33, 35, 40-43, and 47 are amended. No new matter is added. Claims 24, 28, 30, 33-35, 37, 40-43, and 45-51 are presented for examination. Claims 24, 40, and 47 are independent.

Claim amendments

The claims are amended to replace "a communication network" with "the Internet", for reasons discussed below. This element was already recited in claim 42, and is supported as a preferred network throughout the specification.

Applicants' [0009] lines 1-2: *"According to the invention, a symmetrical encryption method is used for the protected data transmission, for example over a public communication network such as the internet."*

The claims are further amended to replace "operational measurement" with "useful data" as discussed later below.

Response to rejections under 35 USC 103(a)

In par. 5 of the office action, Examiner proposes to ignore the first three steps (a, b, c) of Noguchi, and start at step d for comparison with Applicants' claimed invention. Applicant understands Examiner's point; however, this modification is so major that it eliminates the

purpose of Noguchi (visual verification of a public key), therefore is suggested only by hindsight consideration of Applicants' invention. It ignores the fact that Noguchi is inoperable on public networks such as the Internet because he requires the sending and receiving terminal to be side-by-side for direct visual comparison of verification displays on both terminals by a user. Applicant contends that Noguchi's terminals must be side-by-side for this visual comparison unless every user has a photographic memory. This makes Noguchi inoperable in every realistic situation. All of the claims are amended herein to recite "the Internet".

Noguchi col. 4, lines 48-52: *"The distance between both the data send/receive devices is typically less than 10 m, preferably several meters, such that a user can come and go, since the verification data needs to be compared mutually at the verification data output sections of both the data send/receive devices."*

Noguchi col. 9, lines 33-40: *"(c) Users of source A and destination B verify whether verification data X_p and X_x that are displayed in the respective displays are the same. If X_p equals X_x , this means K_x equals K_p , hence it is determined that data integrity is assured for the communication path between source A and destination B."*

In pars. 15-17 of the office action, Examiner omits consideration of the term "operational". However, this term eliminates Gleeson. The claimed "operational measurement of an automation system" is useful data of an operational system, not a specialized stochastic random number per Gleeson. This distinction is made by Applicant as follows:

Applicants' [0042]-[0043]: *"The generation of the stochastic data as a basis for generating the symmetrical keys in the users 102, 104 can be performed here by a stochastic random number generator which uses, for example, the output voltage of a noisy resistance as the stochastic process."*

Alternatively, the data supplied by the data source 116 can also be used as stochastic data as a basis for generating the symmetrical key. This is advantageous in particular when the data source 116 supplies measured values of quantities or parameters that vary over time, of an automation system for example. For example, certain process parameters in an automation system of said kind, such as the temperature, pressure, speed of rotation, etc., are not deterministic, but more or less random with more or less periodic components. A corresponding measured value supplied by the data source 116 can therefore be used as a stochastic datum

for symmetrical key generation, a separate acquisition module 112 or, as the case may be, an additional stochastic process 114 being superfluous in this case.

FIG. 2 shows a corresponding flowchart. Stochastic data is acquired in step 200. In this case said data can be stochastic data supplied by a random number generator or the useful data supplied by a data source."

It is clear from the use of the terms "alternative" and "or" above, that stochastic data supplied by a random number generator is not the same as useful data. For this reason, adding the stochastic random number generator of Gleeson to the teaching of Noguchi does not meet any of the independent claims 24, 40, or 47. This distinction was already present in the claims in the term "operational measurement". However, "operational measurement" has been changed herein to "useful data" or "useful datum" to clarify this element.

Furthermore, claim 24 now recites: *"the first and second users then encrypting and communicating useful data over the Internet using the secret encryption program and the first symmetrical encryption key; and wherein the first random value comprises a digital value derived from the useful data."* This means the first random value is derived from useful communication data. This is supported in Applicants' FIG 4, [0052]-[0059], in which data sources 418, 420, and 422 continuously supply useful data a, b, and c, each of which data stream is measured at a given moment in time [0055] to provide values for key generation. These same data streams a, b, c are then encrypted and transmitted over the network as useful data [0059].

In par. 23 of the office action, Examiner cites Gleeson col. 3, lines 44-62 as teaching that first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval. However, this is not found in the cited lines, which describe chaotic processes that can be probed and measured to form the basis for random numbers. Predetermined times are not mentioned.

In par. 27 of the office action, Examiner cites Noguchi Fig 13, col. 13, lines 48-63 as teaching use of the Internet. However, neither the term "Internet" nor the term "public network" are not found anywhere in Noguchi. His embodiment of Fig 13 does not make his

method usable on the Internet. The two PDA users still must visually verify the verification display by looking at both PDAs, which means they must be side-by-side at the same location.

The method of Noguchi would be impractical to repeat or restart at intervals for security reasons during a communication session, because each repetition would interrupt the users and require them to perform another visual verification.

Regarding claim 41: Examiner asserts that it would be an obvious design choice to use the least significant bits of measured data to generate an encryption key. In par. 39 of the office action, he refers to Petersen par. 39. However par. 39 of Petersen teaches avoiding deletion of high order bits of data, explicitly teaching away from Applicants' method of claim 41. Loss of high order bits is an overflow condition, which is a "fatal" or terminal error, and is displayed as such on all calculators.

Petersen par. 39, lines 6-12 : *"The position of the decimal separator in a fixed-point number is a weighting between digits in the integer part and digits in the fraction part of the number. To achieve the best result of a calculation, it is usually desired to include as many digits after the decimal separator as possible, to obtain the highest resolution. However, it may also be important to assign enough bits to the integer part to ensure that no overflow will occur. Overflow is loading or calculating a value into a register that is unable to hold a number as big as the value loaded or calculated. Overflow results in deletion of the most significant bits (digits) and possible sign change."*

A design choice is one of several known options that are similarly good choices. However, removing high-order bits from useful measurement data destroys the data. For example, assume a time series of 8-bit measurement data has a range from binary 00100101 to 01110011 (decimal 37 to 115). If you remove the top 2 bits, the data is limited to a maximum value of 111111, or decimal 63. This causes an overflow for any values greater than 63, which destroys the data, and thus would certainly not be done without some non-obvious reason. Furthermore, the goal of a random number is unpredictability. The more significant bits there are in a random number, the less predictable and more secure it is as a seed value for an encryption key. This teaches away from using only the least significant bits, either for data or

for security key generation. For these reasons, the method of claim 41 is not supported by general knowledge, and is not an obvious design choice.

MPEP 2142 Legal Concept of *Prima Facie* Obviousness [R-6]: "*The tendency to resort to "hindsight" based upon Applicants' disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.*"

Conclusion

M.P.E.P. 2143.03 provides that to establish prima facie obviousness of a claimed invention, all words in a claim must be considered in judging the patentability of that claim against the prior art. If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.

As argued above, the proposed combinations lack features claimed in the independent claims and others herein, and must be motivated in some cases by hindsight based on Applicants' invention. Thus they do not support the obviousness rejections of the claimed invention. Applicants feel this application is in condition for allowance, which is respectfully requested.

The commissioner is hereby authorized to charge any appropriate fees due in connection with this paper, including fees for additional claims and terminal disclaimer fee, or credit any overpayments to Deposit Account No. 19-2179.

Respectfully submitted,

Dated: March 11, 2009

By: Janet D. Hood
Janet D. Hood
Registration No. 61,142
(407) 736-4234

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830